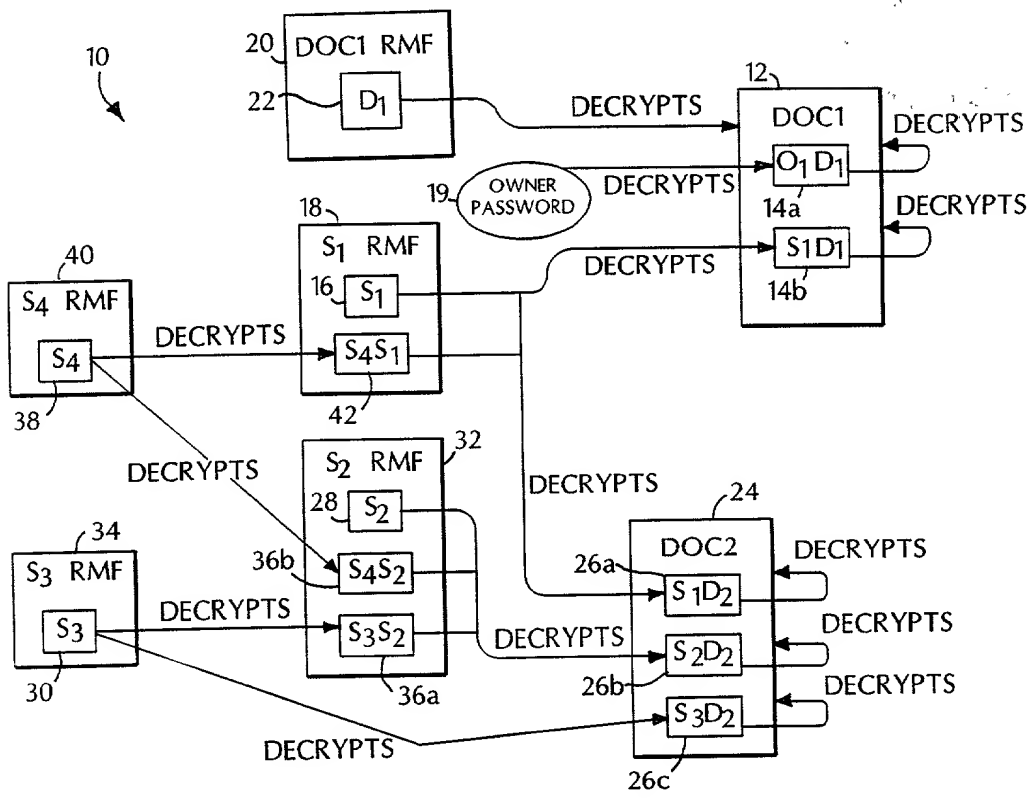

FIG. 1

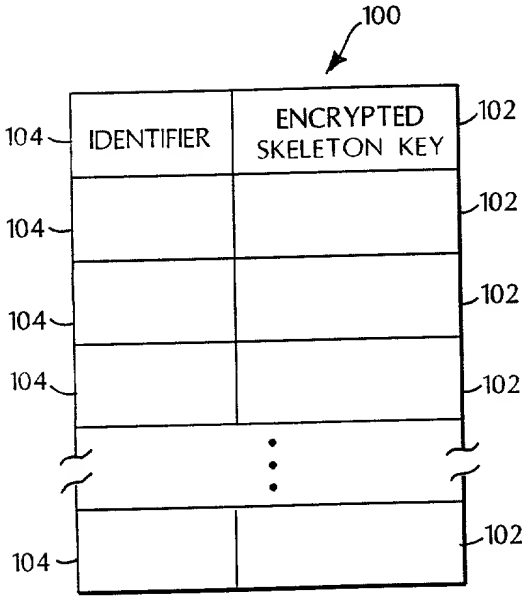

FIG. 4

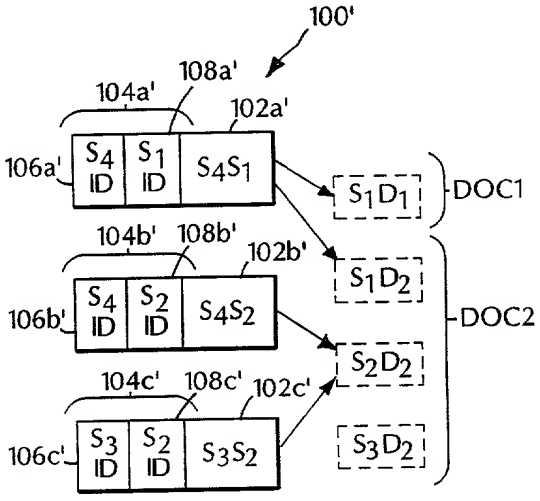

FIG. 5

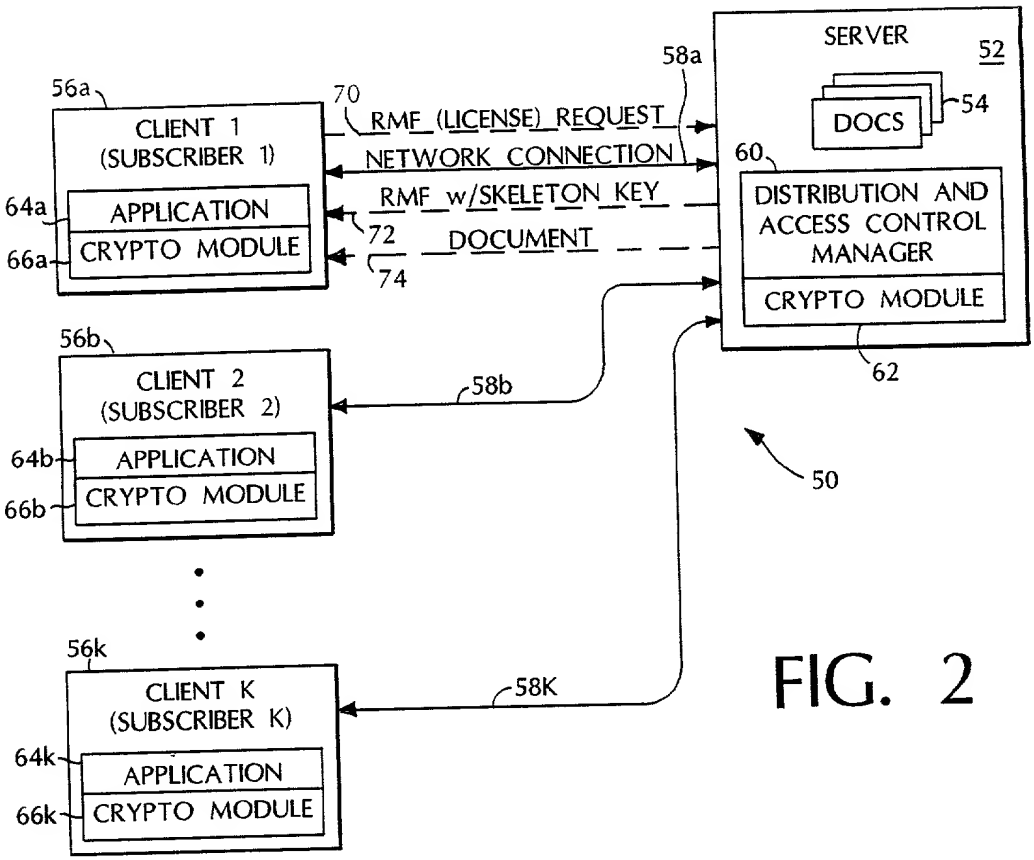
SERVER
52
58a
DOCS
54
56a
70
CLIENT 1
(SUBSCRIBER 1)
RMF (LICENSE) REQUEST
NETWORK CONNECTION
60
64a
APPLICATION
RMF w/SKELETON KEY
DISTRIBUTION AND ACCESS CONTROL MANAGER
66a
CRYPTO MODULE
72
DOCUMENT
74
CRYPTO MODULE
62
56b
CLIENT 2
(SUBSCRIBER 2)
58b
64b
APPLICATION
66b
CRYPTO MODULE
50
56k
CLIENT K
(SUBSCRIBER K)
58K
64k
APPLICATION
66k
CRYPTO MODULE

FIG. 2

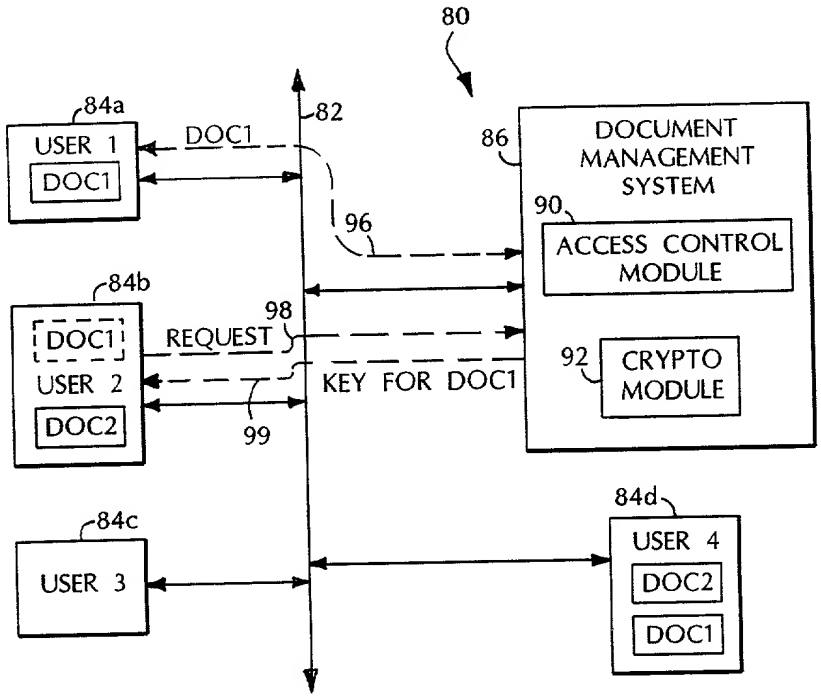
80
84a
USER 1
DOC1
DOC1
82
86
DOCUMENT MANAGEMENT SYSTEM
90
96
ACCESS CONTROL MODULE
84b
DOC1
98
REQUEST
USER 2
DOC2
KEY FOR DOC1
92
CRYPTO MODULE
99
84d
84c
USER 3
USER 4
DOC2
DOC1

FIG. 3

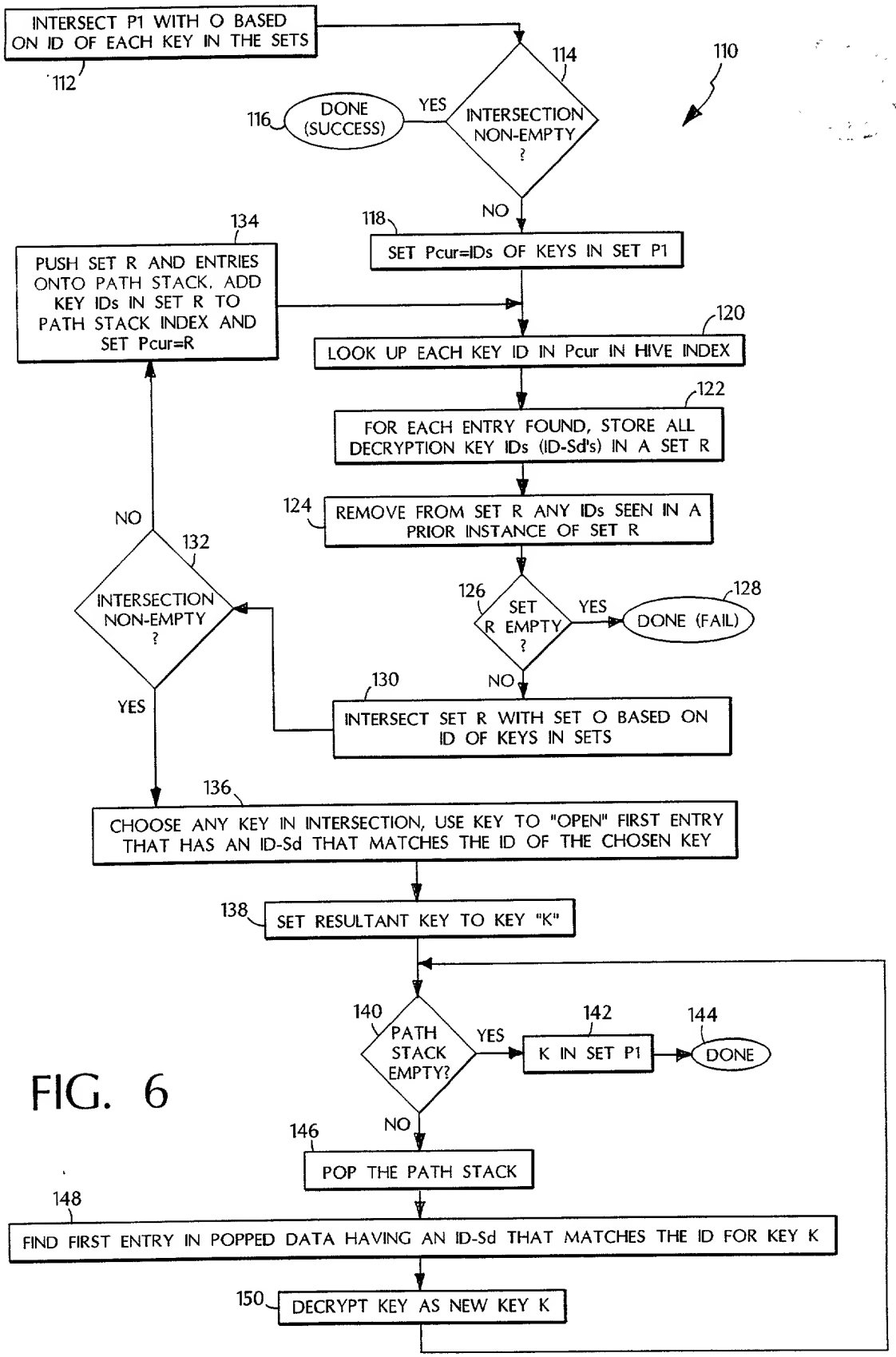
INTERSECT P1 WITH O BASED ON ID OF EACH KEY IN THE SETS
112
114
110
INTERSECTION NON-EMPTY ?
YES
116
DONE (SUCCESS)
NO
118
SET Pcur=IDs OF KEYS IN SET P1
134
PUSH SET R AND ENTRIES ONTO PATH STACK. ADD KEY IDs IN SET R TO PATH STACK INDEX AND SET Pcur=R
120
LOOK UP EACH KEY ID IN Pcur IN HIVE INDEX
122
FOR EACH ENTRY FOUND, STORE ALL DECRYPTION KEY IDs (ID-Sd's) IN A SET R
124
REMOVE FROM SET R ANY IDs SEEN IN A PRIOR INSTANCE OF SET R
126
SET R EMPTY ?
YES
128
DONE (FAIL)
NO
132
INTERSECTION NON-EMPTY ?
NO
YES
130
INTERSECT SET R WITH SET O BASED ON ID OF KEYS IN SETS
136
CHOOSE ANY KEY IN INTERSECTION, USE KEY TO "OPEN" FIRST ENTRY THAT HAS AN ID-Sd THAT MATCHES THE ID OF THE CHOSEN KEY
138
SET RESULTANT KEY TO KEY "K"
140
PATH STACK EMPTY?
YES
142
K IN SET P1
144
DONE
NO
146
POP THE PATH STACK
148
FIND FIRST ENTRY IN POPPED DATA HAVING AN ID-Sd THAT MATCHES THE ID FOR KEY K
150
DECRYPT KEY AS NEW KEY K

FIG. 6